UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/763,773	02/26/2001	Ahmet Mursit Eskicioglu	RCA 89181	5177

7590 05/06/2004

Joseph S Tripoli
Thomson Multimedia Licensing Inc
PO Box 5312
Princeton, NJ 08540

EXAMINER	
WU, ALLEN S	

ART UNIT	PAPER NUMBER
2135	5

DATE MAILED: 05/06/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/763,773	ESKICIOGLU ET AL.	
	Examiner	Art Unit	
	Allen S. Wu	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *26 February 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date 4.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Objections

1. Claim 11 objected to under 37 CFR 1.75(c), as being of improper dependent form for failing to further limit the subject matter of a previous claim. Applicant is required to cancel the claim(s), or amend the claim(s) to place the claim(s) in proper dependent form, or rewrite the claim(s) in independent form. Parent claim 10 recites a "digital video cassette recorder" to be the "recording apparatus". Claim 11 does not further limit the limitation of the recording apparatus by reciting "a recordable DVD apparatus" as the "recording apparatus.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1, 12, and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Park, US Patent 5,689,559, in view of EBU Project Group B/CA (hereinafter EBU), Functional Model of a Conditional Access System.

As per claim 1, Park discloses a method for copying having a scrambled program content component and a control component (see for example; abstract and col 3 ln 61-col 4 ln 8) comprising; receiving, in a recording apparatus, said program (see for example; col 3 ln 61-67); attaching a data item to said control component (see for example; col 3 ln 61-col 4 ln 8and fig 3), said data item

indicating that said program has been copied (see for example; col 3 ln 25-36). The data item (CP information) contains a field indicating the current generation of the copy, thus indicating that the program has been copied. And recording said program content component and nested control component (see for example; col 4 ln 6-19 and col 6 ln 54-62).

As for encrypting said encrypted control component and said data item to generate a nested control component, Park discloses encrypting said data item and control component (see for example; col 4 ln 1-8). Park does not explicitly teach an encrypted control component. EBU further discloses an encrypted control component (see for example; entitlement control message (ECM), page 65 Glossary and page 68 section 3.3). ECMs are well known in the art to be encrypted cryptograms and used to control the descrambling of programs and further add security by enabling conditional access conditions. Therefore, one of ordinary skill in the art at the time of the applicant's invention would have realized the combining of ECM, as the control component, and data item, and to further encrypt the combination to produce the nested control component. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of EBU within the system of Park because it would have increased access security through the use of ECMS as a control component.

As per claim 12, Park discloses managing access to a copy of a restricted program (see for example; abstract) comprising: receiving said restricted program in a processing apparatus (see for example; col 4 ln 45-48), said restricted program having a scrambled program content component (see for example; col 4 ln 45-58) and a nested control component (see for example, marker col 4 ln 49-54), said nested control component being encrypted (see for example; col 4 ln 49-54); decrypting said nested control component (see for example; col 4 ln 49-54) to obtain a control component and a data item (see for example; control word, col 4 ln 54-58 and col 6 ln 21-27). The data item (CP information) contains a field indicating the current generation of the copy, thus indicating that the program has been copied. And recording said program content component and nested control component (see for example; col 4 ln 1-19 and col 6 ln 51-62). Park further discloses obtaining a descrambling key and copy control information (see for example; col 4 ln 54-60); comparing said copy control information and said data item to determine if said copy is valid (see for example; col 5 ln 54-64); and descrambling said program content component, using said descrambling key in response to a determination that said copy is valid (see for example, col 4 ln 18-34 and col 5 ln 56-64).

As for the encrypted control component, Park does not explicitly teach an encrypted control component. EBU further discloses an encrypted control component (see for example; entitlement control message (ECM), page 65 Glossary and page 68 section 3.3) and decrypting the encrypted control

component to obtain a decrypting key (see for example; page 68 section 3.3 paragraphs 1-2). ECMs are well known in the art to be encrypted cryptograms and used to control the descrambling of programs and further add security by enabling conditional access conditions. Therefore, one of ordinary skill in the art at the time of the applicant's invention would have realized the combining of ECM, as the control component, and data item, and to further encrypt the combination to produce the nested control component. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of EBU within the system of Park because it would have increased access security through the use of ECMS as a control component.

As per claim 20, Park discloses managing access to a copy of a restricted program (see for example; abstract) comprising: receiving said restricted program in a processing apparatus (see for example; col 4 ln 45-48), said restricted program having a scrambled program content component (see for example; col 4 ln 45-58) and a nested control component (see for example, marker col 4 ln 49-54), said nested control component being encrypted (see for example; col 4 ln 49-54); decrypting said nested control component (see for example; col 4 ln 49-54) to obtain a control component and a data item (see for example; control word, col 4 ln 54-58 and col 5 ln 21-27). The data item (CP information) contains a field indicating the current generation of the copy, thus indicating that the program has been copied. And recording said program

content component and nested control component (see for example; col 4 ln 1-19 and col 6 ln 50-62). Park further discloses obtaining a descrambling key and copy control information (see for example; col 4 ln 54-60); comparing said copy control information and said data item to determine if said copy is valid (see for example; col 5 ln 54-64); and descrambling said program content component, using said descrambling key in response to a determination that said copy is valid (see for example, col 4 ln 20-34 and col 5 ln 56-64).

As for the encrypted control component, Park does not explicitly teach an encrypted control component. EBU further discloses an encrypted control component (see for example; entitlement control message (ECM), page 65 Glossary and page 68 section 3.3) and decrypting the encrypted control component to obtain a decrypting key (see for example; page 68 section 3.3 paragraphs 1-2). ECMs are well known in the art to be encrypted cryptograms and used to control the descrambling of programs and further add security by enabling conditional access conditions. Therefore, one of ordinary skill in the art at the time of the applicant's invention would have realized the combining of ECM, as the control component, and data item, and to further encrypt the combination to produce the nested control component. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of EBU within the system of Park because it would have increased access security through the use of ECMS as a control component.

As for transferring, from a bank, a cash reserve to said smart card, EBU further discloses use of a smart card in a conditional access system using a payment scheme (see for example; page 69 section 3.4 paragraph 4 and page 72-73 section 5.1), wherein a cash reserve is transferred, from a bank (see for example page 74 paragraph 2), to said smart card (see for example page 73 paragraph 1). As for the verification that a cost of said restricted program is less than the stored cash reserve and deducting the cost of said restricted program from said stored cash reserve. EBU further discloses such a payment scheme wherein viewing tokens are on a smart card (see for example; page 73 paragraph 1). The purpose of such tokens is to pay for the program or event ordered. One of ordinary skill in the art at the time of the applicant's invention would have realized such verification that the cost of said restricted program is less than the stored cash reserve before descrambling the audio/video component is necessary for such a payment scheme to be effective and that payment before descrambling is the objective of such a payment scheme. It would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to combine the payment schemes of EBU within the system of Park because it would have provided a means of collecting payment for services.

4. Claims 2-10 and 13-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Park, US Patent 5,689,559, in view of EBU Project Group B/CA

(hereinafter EBU), Functional Model of a Conditional Access System, and further in view of Mandelbaum et al (hereinafter Mandelbaum), US Patent 5,544,246.

As per claim 2, Park-EBU discloses the claimed limitations as described above (see claim 1 above). EBU further discloses the use of a smart card for performing conditional access functions, such as receiving and descrambling (see for example; page 69 paragraph 6). Park-EBU does not explicitly teach a smart card for encrypting data. Smart cards are well known in the art to provide a plurality of cryptographic functions, including receiving, attaching, and encrypting. Furthermore, smart cards are well known in the art to provide added convenience of being easily replaceable, thus enabling a means of adding new features in a convenient manner. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Mandelbaum within the Park-EBU combination because it would have provided convenience in updating new features or changing encryption keys to promote added security.

As per claim 3, Park-EBU-Mandelbaum discloses the claimed limitations as described above (see claim 2 above). Park further discloses control component comprising of a descrambling key associated with the scrambled program content component (see for example; col 3 ln 61-col 4 ln 8). EBU further discloses the encrypted control component comprising copy information

(see for example; ECM page 68 section 3.3). ECM is well known in the art to contain copy control information to provide conditional access to a system.

As per claim 4, Park-EBU-Mandelbaum discloses the claimed limitations as described above (see claim 3 above). Park further discloses copy control information indicating on of never-copy state and copy-once state (see for example col 3 ln 1-4).

As per claim 5, Park-EBU-Mandelbaum discloses the claimed limitations as described above (see claim 4 above). Park-EBU does not explicitly teach encrypting using a global public key. Mandelbaum further discloses using encryption with a global public key in smart cards (see for example col 6 ln 53-67). Public keys are well known in the art to be secure in that no communication is necessary to reveal any secrets in decrypting an encrypted data. It would have been obvious to one of ordinary skill in the art a the time of the applicant's invention to encrypt the encrypted control component of EBU using a global public key of Mandelbaum because it would have increased security through lower communication on revealing the secret key and less burden of administering secrets among parties.

As per claim 6, Park-EBU-Mandelbaum discloses the claimed limitations as described above (see claim 5 above). Park-EBU does not explicitly teach

encrypting using a global public key. Mandelbaum further discloses using encryption with a global public key in smart cards (see for example col 6 ln 53-67). Public keys are well known in the art to be secure in that no communication is necessary to reveal any secrets in decrypting an encrypted data. It would have been obvious to one of ordinary skill in the art a the time of the applicant's invention to encrypt the nested control component of Park-EBU using a global public key of Mandelbaum because it would have increased security through lower communication on revealing the secret key and less burden of administering secrets among parties.

As per claim 7, Park-EBU-Mandelbaum discloses the claimed limitations as described above (see claim 6 above). Mandelbaum further discloses said global public key being associated with said smart card (see for example; col 6 ln 52-62), said smart card having a corresponding private key stored therein (see for example col 6 ln 52-62).

As per claim 8, Park-EBU-Mandelbaum discloses the claimed limitations as described above (see claim 7 above). EBU further discloses the encrypted control component further comprises purchase information (see for example page 72-73 section 5.1). Channel identification data, event identity data, data and time stamp data, and billing data are well known in the art to be incorporated in such payment schemes and are necessary for the determination of charge

amount and time of charge or production in such payment schemes as pay-per-view. The concept of billing a customer for descrambling and viewing or recording of such programs are well known in the art to provide revenue to providers. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of EBU within the system of Park because it would have further provided a means of charging customers for viewing programs.

As per claim 9, Park-EBU-Mandelbaum discloses the claimed limitations as described above (see claim 8 above). EBU further discloses a smart card comprising a card body with a plurality of terminals arranged on a surface of said card body in accordance with one of ISO 7816 (see for example, page 72 section 4.3 paragraph 1) and PCMCIA card standards (see for example, page 67 section 3.1 paragraph 2).

As per claim 10, Park-EBU-Mandelbaum discloses the claimed limitations as described above (see claim 9 above). Park further discloses a digital video cassette recorder (see for example; DVCR fig 4 and col 7 ln 17-20).

As per claim 13, Park-EBU discloses the claimed limitations as described above (see claim 12 above). Mandelbaum further discloses using encryption with a global public key in smart cards (see for example col 6 ln 53-67). Public

keys are well known in the art to be secure in that no communication is necessary to reveal any secrets in decrypting an encrypted data. It would have been obvious to one of ordinary skill in the art a the time of the applicant's invention to encrypt the nested control component of Park-EBU using a global public key of Mandelbaum because it would have increased security through lower communication on revealing the secret key and less burden of administering secrets among parties.

As per claim 14, Park-EBU-Mandelbaum discloses the claimed limitations as described above (see claim 13 above). EBU further discloses steps of receiving, decrypting, and comparing are performed in a smart card coupled to said processing apparatus (see for example, page 69 section 3.4 paragraph 4). The smart card is used as a conditional access security module (see for example page 67 section 3.1 paragraphs 1-2). One of ordinary skill in the art at the time of the applicant's invention would have realized such comparison being done in the security module (smart card) to relieve processing done by the recording and centralize the security protocols on one security module. Furthermore, smart cards are well known in the art to provide added convenience of being easily replaceable, thus enabling a means of adding new features in a convenient manner. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of EBU within the system of

Park because it would have provided convenience in updating new features or changing encryption keys to promote added security.

Mandelbaum further discloses said a public key scheme wherein the global public key being associated with said smart card (see for example; col 6 ln 52-62), said smart card having a corresponding private key stored therein (see for example col 6 ln 52-62).

As per claim 15, Park-EBU-Mandelbaum discloses the claimed limitations as described above (see claim 14 above). EBU further discloses the encrypted control component further comprises purchase information (see for example page 72-73 section 5.1). Channel identification data, event identity data, data and time stamp data, and billing data are well known in the art to be incorporated in such payment schemes and are necessary for the determination of charge amount and time of charge or production in such payment schemes as pay-per-view. The concept of billing a customer for descrambling and viewing or recording of such programs are well known in the art to provide revenue to providers. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of EBU within the system of Park because it would have further provided a means of charging customers for viewing programs.

As per claim 16, Park-EBU-Mandelbaum discloses the claimed limitations as described above (see claim 15 above). Park discloses descrambling and passing said descrambled transmitted event to said video processing apparatus (see for example; col 7 ln 16-20). EBU further discloses deducting the cost of said program from a cash reserve stored in said smart card to determine a calculated cash reserve (see for example; page 72 paragraphs 1-2) descrambling, in said smart card, said scrambled program content component using said descrambling key (see for example page 69 section 3.4 paragraph 4) in response to having a positive calculated cash reserve (see for example page 73 paragraph 1). The use of cash reserve and deducting the cost of a paid program is well known the art in digital payment broadcast schemes. Furthermore, the purpose of such payment schemes is to prevent descrambling if there is no payment, i.e. insufficient funds. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of EBU within the system of Park because it would have provided a scheme in collecting payment for viewing programs.

As per claim 17, Park-EBU-Mandelbaum discloses the claimed limitations as described above (see claim 16 above). As for an e-cash certificate message from an automatic teller machine. EBU further discloses a payment scheme wherein cash is downloaded into the smart card as "cash tokens" (see for example; page 73 paragraph 1). The downloading of a cash certificate (cash

token) must come from some credible source, which is well known in the art to be automated teller machines. One of ordinary skill in the art at the time of the applicant's invention would have realized that such downloading must of come from an automatic teller machine in order for the cash certificate to be credible for use in such a payment scheme.

As per claim 18, Park-EBU-Mandelbaum discloses the claimed limitations as described above (see claim 17 above). Park further discloses a processing apparatus is one of a digital video cassette recorder/player and a DVD recorder/player (see for example; col 7 ln 16-20).

As per claim 19, Park-EBU-Mandelbaum discloses the claimed limitations as described above (see claim 18 above). EBU further discloses a smart card comprising a card body with a plurality of terminals arranged on a surface of said card body in accordance with one of ISO 7816 (see for example, page 72 section 4.3 paragraph 1) and PCMCIA card standards (see for example, page 67 section 3.1 paragraph 2).

5. Claim 11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Park, US Patent 5,689,559, in view of EBU Project Group B/CA (hereinafter EBU), Functional Model of a Conditional Access System, in view of Mandelbaum et al (hereinafter

Mandelbaum), US Patent 5,544,246, and further in view of Kuroda et al, US Patent 5,815,472.

As per claim 11, Park-EBU-Mandelbaum discloses the recording apparatus as described above (see claim 10). Park-EBU-Mandelbaum does not explicitly teach the recording apparatus being a DVD recorder. Kuroda discloses a DVD recorder for recording and reproducing data (see for example; col 8 ln 28-34). DVDs are well known in the art to be used for holding high quality digital media due to the amount of storage space on the disk and further are a popular form of external storage. It would have been obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings of Kuroda within the combination of Park, EBU, and Mandelbaum because it would have provided a storage media that is popular in use and known for high quality and capacity of digital media.

Conclusion

6. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Kim et al, US Patent 5,799,081, discloses a copy protection method for prohibiting unauthorized copying.

Bradley et al, US Patent 4,878,245 discloses a method of payment for descrambling of digital broadcasts.

Pitts et al, US Patent 4,893,248, discloses payment information in a digital broadcast for charge determination.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Allen S. Wu whose telephone number is 703-305-0708. The examiner can normally be reached on Monday-Friday 9am-5pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 703-305-4393. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Allen Wu
Patent Examiner
Art Unit 2135

ASW

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100